INDIRE ISTITUTO NAZIONALE DOCUMENTAZIONE INNOVAZIONE RICERCA EDUCATIVA

FORMAZIONE

FUTURA PNRR ISTRUZIONE LA SCUOLA PER L'ITALIA DI DOMANI

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Istruzione e del Merito

PERSONALE ATA

Proteggere i dati personali e la privacy

Tiziana Viti

COLLABORATORI · OPERATORI · ASSISTENTI · TECNICI

LE NOVITÀ DEL DIGCOMP 2.2. E I CAMPI DI APPLICAZIONE

LE CINQUE AREE

1. Alfabetizzazione su informazioni e dati
2. Comunicazione e collaborazione
3. **Creazione di contenuti digitali**
4. Sicurezza
5. Risolvere problemi

OBIETTIVO GENERALE è fare in modo che tutti i dipendenti pubblici siano in grado di operare attivamente in modo sicuro, consapevole, collaborativo e orientato al risultato all'interno di una pubblica amministrazione sempre più digitale. si concentra esclusivamente sugli aspetti pertinenti alle competenze digitali complementari richieste ad un dipendente pubblico che lavora in ambienti digitali

Il **DigComp** è stato adottato a livello europeo per costruire il "Digital Skills Indicator", l'indice delle competenze digitali, utilizzato per definire gli obiettivi politici e monitorare il "Digital Economy and Society" (DESI), l'Indice dell'Economia e della Società Digitale. *"attualizza aspetti essenziali per la definizione di competenza digitale e fornisce più di 250 nuovi esempi di conoscenze, abilità e attitudini che aiutano i cittadini a impegnarsi con facilità, in modo critico e sicuro con le tecnologie digitali e con quelle nuove ed emergenti, come i sistemi guidati dall'intelligenza artificiale, il lavoro a distanza, l'accessibilità.*

Alfabetizzazione su informazioni e dati	1.1. Navigare, ricercare e filtrare dati, informazioni e contenuti digitali 1.2. Valutare dati, informazioni e contenuti digitali 1.3. Gestire dati, informazioni e contenuti digitali
Comunicazione e collaborazione	2.1. Interagire con gli altri attraverso le tecnologie 2.2. Condividere informazioni attraverso le tecnologie digitali 2.3. Esercitare la cittadinanza attraverso le tecnologie digitali 2.4. Collaborare attraverso le tecnologie digitali 2.5. Netiquette 2.6. Gestire l'identità digitale
Creazione di contenuti digitali	3.1. Sviluppare contenuti digitali 3.2. Integrare e rielaborare contenuti digitali 3.3. Copyright e licenze 3.4. Programmazione
Sicurezza	4.1. Proteggere i dispositivi 4.2. Proteggere i dati personali e la privacy 4.3. Proteggere la salute e il benessere 4.4. Proteggere l'ambiente
Risolvere problemi	5.1. Risolvere problemi tecnici 5.2. Individuare bisogni e risposte tecnologiche 5.3. Utilizzare in modo creativo le tecnologie digitali 5.4. Individuare i divari di competenze digitali

CATEGORIE DI DATI SECONDO IL GDPR

Norme di riferimento

- **Regolamento UE 2016/679 (GDPR)** – Articoli 4, 6, 9, 10
- **D.Lgs. 196/2003** aggiornato dal **D.Lgs. 101/2018**
- **Linee guida del Garante Privacy per la scuola**: https://www.garanteprivacy.it/home/temi/scuola

Categoria	Definizione normativa	Esempi scolastici	Base giuridica e riferimenti
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile (art. 4, par. 1 GDPR)	Nome, cognome, indirizzo, codice fiscale, numero di matricola, fotografia	Art. 6 GDPR – Liceità del trattamento
Dati particolari (ex "sensibili")	Dati che rivelano origine razziale/etnica, opinioni politiche, convinzioni religiose, stato di salute, vita sessuale, dati biometrici o genetici (art. 9 GDPR)	Certificati di disabilità, allergie alimentari, religione per scelta mensa, appartenenza sindacale	Art. 9 GDPR – Trattamento solo in casi specifici e con garanzie
Dati giudiziari	Dati relativi a condanne penali e reati o misure di sicurezza (art. 10 GDPR)	Casellario giudiziale per assunzioni, sospensioni disciplinari gravi, segnalazioni dal tribunale dei minori	Art. 10 GDPR – Solo se previsto da norme di legge
Dati anonimi / pseudonimizzati	Dati non riferibili direttamente a una persona (anonimi) o modificati per limitarne l'identificabilità (pseudonimi)	Analisi statistiche anonime sugli esiti scolastici; numeri identificativi cifrati	Recital 26 GDPR – Fuori ambito se realmente anonimi

IL GDPR SI FONDA SU DIVERSI PRINCIPI TUTTI SUSSUMIBILI NEL CONCETTO DI ACCOUNTABILITY : I PRINCIPI DEVONO ESSERE TRASPOSTI IN COMPORTAMENTI CONCRETI DA PARTE DEL TITOLARE

si traduce come **responsabilizzazione**: significa che il titolare del trattamento (es. dirigente scolastico) **non solo deve rispettare il GDPR**, ma **deve dimostrare in modo attivo e documentato** di averlo fatto.

"Il titolare del trattamento è responsabile del rispetto dei principi e deve essere in grado di comprovarlo."— **Art. 5, par. 2 GDPR**

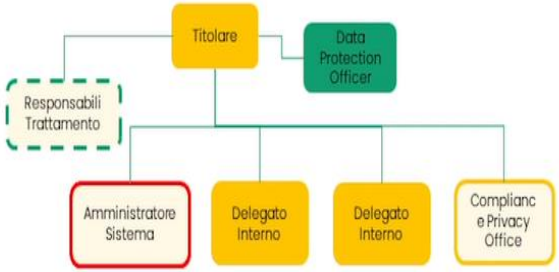
DOCUMENTI TIPICI DI UNA SCUOLA "ACCOUNTABLE"

- **Registro trattamenti**
- **Consensi informati e liberatorie**
- **Nomine a responsabili esterni (es. Google Workspace, Axios)**
- **Manuale privacy interno**
- **Report DPIA per servizi cloud, app, videosorveglianza**
- **Attestati di formazione del personale**
- **Procedura per la gestione dei data breach**

Riferimento	Contenuto
Art. 5, par. 2 GDPR	Principio di accountability: obbligo di dimostrare la conformità
Art. 24 GDPR	Responsabilità del titolare nel mettere in atto misure tecniche e organizzative adeguate
Art. 25 GDPR	Privacy by Design e Default come strumenti di accountability
Art. 30 GDPR	Registro delle attività di trattamento come prova
Art. 32 GDPR	Obbligo di sicurezza dei dati

POLICY

Prioritario **definire** internamente ruoli e responsabilità.



Adottare un regolamento che definisca **regole** di comportamento da seguire per approcciare in maniera corretta al trattamento dati.

Prevedere politiche di **Data Retention** e **Minimizzazione**.

Ruolo	Funzione	Norma di riferimento
Titolare del trattamento	Decide *finalità* e *mezzi* del trattamento dati	Art. 4.7 – Art. 24 GDPR
Responsabile della protezione dati (DPO)	Figura di garanzia e consulenza per GDPR, obbligatoria in enti pubblici	Art. 37–39 GDPR
Responsabili esterni	Trattano dati per conto della scuola (software, cloud, etc.)	Art. 28 GDPR
Referente privacy interno	Supporta il dirigente nella gestione operativa	Non previsto da GDPR, ma prassi utile
Personale autorizzato	Dipendenti che trattano dati previa formazione e istruzioni scritte	Art. 29 GDPR

LE PRINCIPALI **CONTROMISURE PER LA PROTEZIONE DEI DATI** (IN OTTICA GDPR),

Controllo degli accessi e gestione permessi
Descrizione: definire ruoli chiari (controller, processor), gestire con log e password la visibilità dei dati.
Esempio scolastico: solo il personale autorizzato (es. segreteria) può accedere al registro elettronico, mentre docenti accedono solo alle proprie classi.

Crittografia e protezione fisica/logica
Descrizione: cifrare dati su chiavette, hard disk, backup; usare firewall, antivirus, IDS/NIDS.
Esempio scolastico: la copia del registro su pendrive è cifrata e riposta in cassaforte; dispositivi scolastici hanno antivirus aggiornati.

LE PRINCIPALI **CONTROMISURE PER LA PROTEZIONE DEI DATI** (IN OTTICA GDPR),

Privacy by Design e Privacy by Default

Descrizione: progettare sistemi e processi considerando la tutela della privacy già nella fase di ideazione; impostazioni di default garantiscono il livello più alto di sicurezza e minimizzazione dei dati.

Esempio scolastico: il software di gestione voti è configurato affinché visualizzi solo i dati necessari (es. nome, classe, voto), senza mostrare informazioni sensibili come allergie o religione.

Minimizzazione dei dati e limitazione della conservazione

Descrizione: raccogliere solo i dati strettamente necessari per uno scopo definito e conservarli il tempo necessario.

Esempio scolastico: raccogliere il solo recapito email per le comunicazioni scolastiche, cancellarlo dopo tre anni dalla fine della scuola; oppure attendere l'autorizzazione per foto o dati speciali.

LE PRINCIPALI **CONTROMISURE PER LA PROTEZIONE DEI DATI** (IN OTTICA GDPR),

Valutazione d'impatto (DPIA)

Descrizione: analisi formale del rischio privacy prima di trattamenti ad alto impatto (es. biometria, cloud estero, profiling).

Esempio scolastico: valutazione pre-installo di sistemi di riconoscimento automatico delle presenze (facial recognition), che può essere illegale senza DPIA.

Gestione delle violazioni e data breach

Descrizione: procedure di notifica, analisi rapide e documentazione in caso di violazioni o accessi non autorizzati.

Esempio scolastico: se un docente dimentica un PC con dati in classe, lo si segnala entro 72h al responsabile e si avvia investigazione.

Controlli su terze parti e contratti con responsabili esterni

Descrizione: verificare la conformità GDPR di fornitori ICT (cloud, app), stabilire contratti che facciano esplicito riferimento alla protezione dati.

Esempio scolastico: prima di usare app di quiz online, si richiede accordo scritto GDPR e si rivede la privacy policy.

📜 Diritti dell'interessato sui dati personali (Articoli 15–22 GDPR)

Diritto	Descrizione	Esempio scolastico
1. Diritto di accesso (art. 15)	Ottenere conferma che sia in corso un trattamento dei propri dati e accedere ai dati stessi	Un genitore chiede di vedere i dati contenuti nel registro elettronico riferiti al figlio
2. Diritto di rettifica (art. 16)	Correggere dati personali inesatti o incompleti	Uno studente segnala un errore nel proprio indirizzo o nel codice fiscale
3. Diritto alla cancellazione ("diritto all'oblio") (art. 17)	Ottenere la cancellazione dei dati in determinati casi (es. se non più necessari)	Dopo il diploma, un ex alunno chiede la cancellazione dei propri dati dal sito web della scuola
4. Diritto alla limitazione del trattamento (art. 18)	Sospendere temporaneamente il trattamento in caso di contestazione sull'esattezza o liceità	Un docente chiede la sospensione della diffusione dei propri dati finché non viene risolta una controversia
5. Diritto alla portabilità dei dati (art. 20)	Ricevere i propri dati in formato strutturato e trasmetterli ad altro titolare	Un genitore chiede il trasferimento dei dati scolastici del figlio a una nuova scuola in formato digitale
6. Diritto di opposizione (art. 21)	Opporsi, per motivi legittimi, al trattamento dei dati	Un docente si oppone alla pubblicazione online del proprio orario di servizio nominativo
7. Diritto a non essere sottoposto a decisioni automatizzate (art. 22)	Non essere oggetto di decisioni basate solo su trattamenti automatizzati senza intervento umano	Uno studente contesta un'esclusione da una graduatoria generata automaticamente da un software

LE PRINCIPALI **CONTROMISURE PER LA PROTEZIONE DEI DATI** (IN OTTICA GDPR),

Registro delle attività di trattamento (RPA)

Descrizione: Censire ovvero tracciare formalmente i processi di trattamento dati, come richiesto dall'art. 30 GDPR.

Esempio scolastico: elenco dei database scolastici, applicazioni usate e categorie di dati trattati, con date e responsabili.

Formazione del personale e consapevolezza

Descrizione: training su phishing, social engineering, gestione privacy e procedure GDPR.

Esempio scolastico: docente segnala email sospette e partecipa a corso "sicurezza informatica per scuole".

Informativa e consenso trasparenti

Descrizione: fornire chiare informative a studenti/famiglie su dati raccolti, uso e destinatari, ottenere consenso esplicito quando necessario.

Esempio scolastico: al momento delle foto per sito web, si consegna un foglio informativo da firmare da genitori.

.

SINTESI DELLE CONTROMISURE

Misura	Finalità	Esempio scolastico
Privacy by Design	Strutturare privacy da progetto	Registro con dati minimali
Minimizzazione	Evitare dati superflui	Email comunicazioni, niente foto non autorizzate
Accessi controllati	Sicurezza logici/fisici	Solo docenti classi e segreteria per attività A e B
Crittografia	Evitare accessi non autorizzati	Pendrive cifrata
Formazione	Consapevolezza staff	Corsi anti-phishing
Informativa & consenso	Trasparenza e legalità	Fogli genitori per foto/schede
Registro trattamento	Documentazione obbligatoria	Elenco trattamenti dati scolastici
DPIA	Riduzione rischi gravità	Riconoscimento facciale e cloud estero
Data breach	Gestione incidenti	Segnalazione entro 72h
Terze parti	Controllo responsabili	Contratti GDPR con fornitori
Pseudonimizzazione	Privacy nei dati aggregati	Iniziali in wall chart

Contromisura	Descrizione	Esempio scolastico	Normativa di riferimento
1. Privacy by Design e by Default	Protezione integrata nei processi e nei sistemi, con impostazioni predefinite orientate alla minimizzazione dei dati.	Il registro elettronico mostra solo i dati essenziali (es. nome, voto, classe).	GDPR art. 25
2. Minimizzazione e limitazione della conservazione	Raccolta solo di dati necessari e conservazione per il tempo strettamente utile.	Raccogliere solo l'email dei genitori e cancellarla 5 anni dopo l'uscita dello studente.	GDPR art. 5, par. 1, lett. c) e e)
3. Controllo degli accessi e gestione dei ruoli	Limitare l'accesso ai dati solo a chi è autorizzato, in base a compiti e responsabilità.	Il docente accede solo ai dati della sua classe; la segreteria a tutto l'archivio.	GDPR art. 32, co. 1, lett. b)
4. Crittografia e protezione logica/fisica	Protezione dei dati mediante cifratura, antivirus, backup e firewall.	Le chiavette USB con dati degli alunni sono cifrate.	GDPR art. 32, co. 1, lett. a e d)
5. Formazione del personale	**Obbligo di formazione continua su privacy, sicurezza, uso corretto dei dati.**	**Corso annuale per il personale ATA e docenti su GDPR e phishing.**	**GDPR art. 39, co. 1, lett. b); D. Lgs. 196/2003 art. 2-quaterdecies**

Contromisura	Descrizione	Esempio scolastico	Normativa di riferimento
6. Informativa e consenso	Obbligo di fornire un'informativa chiara sul trattamento e ottenere il consenso quando richiesto.	Foglio informativo firmato dai genitori prima della pubblicazione di foto sul sito web.	GDPR art. 13 e 14 (informativa); art. 6, par. 1, lett. a) (consenso)
7. Registro delle attività di trattamento (RPA)	Documento che elenca tutti i trattamenti di dati svolti da una scuola.	Registro contenente descrizione dei software scolastici, finalità e destinatari dei dati.	GDPR art. 30
8. Valutazione d'impatto (DPIA)	Analisi preventiva dei rischi nei trattamenti ad alto impatto.	Prima dell'adozione del riconoscimento facciale per l'ingresso, si effettua una DPIA.	GDPR art. 35
9. Gestione dei data breach	Procedure per notificare entro 72 ore le violazioni di dati personali.	Un tablet con dati scolastici viene smarrito: si attiva la procedura di notifica.	GDPR art. 33 e 34
10. Controllo dei fornitori (responsabili esterni)	Verifica della conformità GDPR dei fornitori, con stipula di contratti scritti.	Contratto con l'azienda che fornisce il software gestionale scolastico.	GDPR art. 28
11. Pseudonimizzazione e offuscamento	**Sostituzione di dati identificabili con codici o altri strumenti per limitare il rischio.**	**Per pubblicare statistiche sugli esiti scolastici si usano codici al posto dei nomi.**	**GDPR art. 32, co. 1, lett. a); art. 4, punto 5**

TABELLA – RESPONSABILITÀ PRIVACY PER COLLABORATORI E OPERATORI SCOLASTICI

Prima posizione economica	Profilo collaboratore e operatore
Custodia e vigilanza su registri, fascicoli e archivi cartacei	Non lascia documenti incustoditi, controlla accesso agli armadi o locali con dati
Segnalazione di data breach o anomalie	Riferisce subito a DSGA/DPO accessi non autorizzati o smarrimenti
Diffonde la coltura privacy	Non diffonde informazioni su studenti o colleghi (es. disabilità, note disciplinari, farmaci)
Supporto nella gestione dei flussi digitali protetti (es. scansioni, fax)	Non salva file in cartelle condivise non protette, distrugge correttamente documenti cartacei
Supporto alla sorveglianza di ambienti video-sorvegliati	Comprende che l'uso delle telecamere ha finalità di sicurezza, non di controllo del personale

Operatore scolastico con mansioni speciali (azienda agraria)	Responsabilità specifica	Descrizione operativa
Raccolta e trattamento di dati biometrici o tecnici (es. sensori clima, telemetria serre)	Gestisce strumentazione automatizzata rispettando i protocolli di sicurezza	Art. 32 GDPR, Regolamento interno sicurezza informatica
Conservazione dati operativi su dispositivi elettronici (es. app, software di monitoraggio)	Non copia i dati su dispositivi non autorizzati (USB personali, cloud esterni)	Regolamento scolastico ICT, Regole sull'accountability
Collaborazione nella documentazione per tracciabilità produzione (es. spirulina, filiere agricole)	Compila documenti garantendo l'integrità e la tracciabilità	Codice Privacy, Registro trattamenti se nominato come incaricato
Interazione con esterni (clienti, enti certificatori)	Rispetta le norme sulla riservatezza e non diffonde dati aziendali o scolastici	Codice Privacy, regolamento scolastico
Custodia delle credenziali informatiche assegnate	Utilizza solo password individuali e non le comunica a terzi	Linee guida AgID, policy interna sicurezza

SITOGRAFIA TEMATICA	Contenuti principali
www.garanteprivacy.it	Portale ufficiale con normativa, provvedimenti e FAQ specifiche per la scuola.
Scuola & Privacy (MIUR)	Sezione del Ministero con linee guida, informative tipo, note operative.
Eur-Lex (portale UE)	Testo integrale e aggiornato del GDPR in italiano.
ForumPA – articoli sulla privacy nella PA	Approfondimenti e buone pratiche nella pubblica amministrazione e nella scuola.
AgID – Linee guida sicurezza	Norme tecniche su sicurezza e trattamento dei dati nella PA.
Generazioni Connesse	Educazione digitale e privacy a scuola (progetto MIUR – EU).

BUON LAVORO !

Dott.ssa Tiziana Viti